E L0 5 ? 9 8 5 7 23 ∪ >

PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06, 29/12, 12/46	A1	(11) International Publication Number: WO 00/08818
		(43) International Publication Date: 17 February 2000 (17.02.00)

(21) International Application Number: PCT/US99/17281

(22) International Filing Date: 30 July 1999 (30.07.99)

(30) Priority Data:
09/128,055   3 August 1998 (03.08.98)   US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, Palo Alto, CA 94303 (US).

(72) Inventor: MONTENEGRO, Gabriel, E.; 6040 Roma Terrace, Fremont, CA 94555 (US).

(74) Agents: HYMAN, Eric, S. et al.; Blakely, Sokoloff, Taylor & Zafman, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025-1026 (US).

(81) Designated States: AE, AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CHAINED REGISTRATIONS FOR MOBILE IP

(57) Abstract

What is disclosed is a method for negotiating access to a private network for a mobile node that has migrated beyond the private network. A plurality of tunnel segments are composed with these tunnel segments composing a chain of a registration request from the mobile node to the private network.

CHAINED REGISTRATIONS FOR MOBILE IP

<u>BACKGROUND OF THE INVENTION</u>

1.   <u>Field of the Invention</u>

The invention relates generally to the field of
communications. More specifically, the invention relates to
computer networking.

2.   <u>Description of the Related Art</u>

For mobile access, particularly where a laptop or other
mobile information device is used, a designation known as
"Mobile IP (Internet Protocol)" has been developed. The
Mobile IP protocol allows a user to "roam" from IP location
to IP location by leaving a "forwarding" address where the
user may be reached (i.e. where IP packets may be forwarded
to), but currently ignores firewalls. Currently, Mobile IP
defines three entities--a mobile node, a home agent and a
foreign agent. The mobile node is the roaming client that
seeks access into the network as if the mobile node were
still within its confines in terms of its IP address.
Through Mobile IP, the mobile node will be able to use a
permanent IP address that it is assigned within the intranet
when it is physically "home" regardless of where in terms of
actual IP address the mobile node may have moved. Through a
process known as registration, a forwarding address is left
with the home agent. The home agent intercepts all packets
destined for the mobile node and sends them to a "foreign
agent" that is currently being visited by the mobile node.
By adding another IP header to packets bound for the mobile
node, the routing system will view the home agent as the
source and the foreign agent as the destination. Once at
the foreign agent the packet can be delivered directly via
data link mechanisms to the mobile node without resorting to
resolving IP headers and without having to perform ordinary
network layer routing.

In order for the home agent to have such a relationship with the foreign agent, the home agent and foreign agent must be directly reachable (i.e. without having to first traverse through a firewall or other impeding node). In many instances, such direct access is not desirable or not possible. For instance, if a mobile node is connecting (gaining Internet access) through an ISP (Internet Service Provider) which acts as the foreign agent, then it may be a breach of security to allow the ISP direct access to the home agent which presumably is located in the premises of a private network or intranet. From the standpoint of the private network, granting such access becomes cumbersome since a mobile node may connect through multiple and different ISPs. The problem is magnified when considering that more than one user may be mobile and attempting to gain remote access via a Mobile IP technique.

Mobile IP, as employed in the current state of the art, assumes that a single registration sets up a "tunnel" (i.e., data pathway) between the mobile node and the home agent Mobile IP assumes that the endpoints of the tunnel are mutually-trusting entities that can and are willing to share registration packets. It also assumes that the mobile node initiates the registration request.

However, in the remote access situation where the access is by a mobile node that has migrated outside a firewall, there may be several intervening entities, such as an ISP, which are not secure, trusting entities. Thus, there is a need for a mechanism that can allow a mobile node, regardless of the number, type of intermediary entities to the private network, to obtain a secure registration. Further, in a mobile node that normally obtains its "home" address, i.e., its IP address when within the private network through assignment by a server (such as DHCP), there is needed a home address discovery mechanism when the mobile node migrates beyond the private network.

SUMMARY OF THE INVENTION

A tunneling set-up protocol is defined so that the registration process may be chained in a compound tunnel which is composed of a plurality of segments. Each tunnel segment composes a registration request passing this along to the next tunnel segment until the endpoint is reached, at which point the registration request of a mobile node may be authenticated for data access to the endpoint. Further, a home address discovery mechanism provides a mobile node with the ability to discover its intranet IP address even though it has migrated beyond the intranet.

BRIEF DESCRIPTION OF THE DRAWINGS

The objects, features and advantages of the method and apparatus for the present invention will be apparent from the following description in which:

Figure 1 is a topological diagram illustrating the operation of chained registrations according to at least one embodiment of the invention.

Figure 2 is a diagram illustrating an exemplary data packet transfer between a mobile node and a correspondent node.

Figure 3 is a diagram illustrating the extensibility of a chained registration technique.

Figure 4 is a flowchart of the chained registration technique according to at least one embodiment of the invention.

Figure 5 illustrates a registration request and reply over the Internet according to one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

Referring to the figures, exemplary embodiments of the invention will now be described. The exemplary embodiments are provided to illustrate aspects of the invention and should not be construed as limiting the scope of the invention. The exemplary embodiments are primarily

3

described with reference to block diagrams or flowcharts. As to the flowcharts, each block within the flowcharts represents both a method step and an apparatus element for performing the method step. Depending upon the implementation, the corresponding apparatus element may be configured in hardware, software, firmware or combinations thereof.

Mobile IP defines the following terms with regard to remote access:

mobile node: The node attempting to register with the network, on whose behalf a compound tunnel may be established.

home agent: The agent which terminates the compound tunnel, and which encapsulates datagrams for the mobile node. The home agent is part of the network which a mobile node would attempt access to, and which ordinarily encapsulates datagram for the mobile node when that node is located within that network.

Figure 1 is a topological diagram illustrating the operation of chained registrations according to at least one embodiment of the invention. A mobile node (MN) 110 may physically migrate from within the premises of a private network 150 to somewhere beyond the private network 150. For instance, MN 110 could be a laptop which is at one point connected to and receives an address from the private network 150. Later, MN 110 may roam somewhere on Internet 130 and thus be outside the segregated confines of the private network 150. When it moves, its actual IP address will no longer be the same as when the MN 110 resided in the private network 150. In attempting to gain access to the private network, a system of registration which is secure and scalable must be provided. The private network 150 is shielded from outside intruders by the use of gateway 140. Gateway 140 is typically a two-way security mechanism that attempts to limit access to the private network and also access from within the private network to the outside. In so doing, the gateway 140 may be responsible for

implementing and administering security, acting as proxy and so forth.

In one embodiment of the invention, a chained registration mechanism is provided which operates as follows. MN 110, when it has moved beyond the private network 150, may be connected to the Internet 130 through a Foreign Agent (FA) 120 such as an ISP (Internet Service Provider). The MN 110 will first send a registration request to FA 120 which contains within it information pertaining to a "care-of-address" (COA) and a "home agent address" (HA). In the exemplary topology of Figure 1, the MN's registration request would identify the gateway A40 to be the HA, because it is the gateway that will identify a home address that is directly reachable from the gateway 140. The request would also contain a COA which shows how the mobile node can be reached. Initially, the MN would be reachable via an IP address assigned by the ISP (FA 120), and thus the FA 120 is listed as the COA.

The FA 120 is the recipient of the registration request and since it will not be allowed to complete the registration request itself (unless the ISP were somehow given secure access to the private network 150, which is typically undesirable), the request is forwarded to the gateway 140 which is designated as the HA. The gateway 140 is not a "home agent" as the term is used in the art since it does not belong to the same subnet as the mobile node (the "home agent" usually refers to an address on the same subnet systems in the same subnet can reach each other by link-layer mechanisms, without recourse to routing. The gateway 140 verifies an authentication which would accompany the registration request and also decodes the addressing information within the registration request. Upon decode, the gateway 140 recognizes that it is designated as the home agent. However, this is not really the case. The gateway 140 can check a database from which it determines that a node 151 is the true "home agent" for the MN 110. The MN 110 would have resided within the subnet in the private

network with node 151 as its home agent. If so, the gateway
140 when presented with the registration request will
initiate an authenticated registration exchange with node
·151. Thus, the registration is "chained" from the MN to the
gateway and then from the gateway to node 151, the true home
agent.

To achieve this chained registration, the gateway 140
composes its own registration request. In this registration
request, the home address will be designated as MN, the node
151 will be designated as the home agent (HA) (which it
truly is), while the gateway 140 will be designated as the
COA. In the special case where the gateway is the true home
agent for the MN 110, then secure remote access will be
achieved upon the completed processing of the first
registration request and the authentication registration
exchange which accompanies it. The true home agent (node
151) verifies the authentication for this registration and
recognizes its validity. The home agent then is able to
establish a secure "tunnel" between the mobile node 110's
packets with the gateway 140. This allows data transfer
between a "correspondent" node(s) within the private network
150 and the mobile node 110, further illustrated in
Figure 2.

Figure 2 is a diagram illustrating an exemplary data
packet transfer between a mobile node and a correspondent
node.

The invention, in various embodiments, permits a mobile
node that has migrated outside of the auspices of a private
network such as a corporate intranet to communicate with
nodes that still reside physically and topologically within
the private network (correspondent nodes). When
correspondent node (for instance, node 152 in Figure 1) and
mobile node (for instance, mobile node 110 in Figure 1)
desire packet transfer a successful chained registration
will first need to occur. After such a registration, data
transfer will occur as follows.

When a correspondent node (whose address is CN) desires
to send a packet of information to a mobile node (whose
address is MN), first, the correspondent node will compose a
packet with a source address of CN and destination address
of MN. The address MN refers to the address of the mobile
node when within the private network, i.e., its permanent
home address. The home agent, whose address is designated
as HA, is a node within the private network which intercepts
this packet link-layer mechanisms like proxy arp and
gratuitous arp or additionally by being the router into that
subnet and forwards it to the FA (whose address is GW). The
home agent will pre-pend an additional header which has a
source address of HA and a destination address of GW. The
gateway then receives this packet and strips the added
header to recover the original packet which has a source
address of CN and destination address of MN. The gateway
will recognize that MN has a "binding" (i.e., a stamp
indicating a valid registration) with a current address of
FA.

The discovery of a binding causes the gateway to
respond by pre-pending its own IP header to the packet that
has as source the address GW and as destination the address
FA, which is the address of the foreign agent (see
Figure 1). The foreign agent obtains the packet, strips
this pre-pended header and recovers the original packet with
source address CN and destination address MN. The foreign
agent recognizes that the packet has the valid binding or
registration and forwards the packet to the mobile node
without additional overhead. The foreign agent can directly
reach the mobile node (by virtue of the mobile node pre-
establishing a link-layer connection with the foreign agent)
and thus, does not need any additional header for routing.
The mobile node receives the packet with the original source
CN and destination address MN specified, and without any
additional addressing headers. Thus, mobility is
transparent; the mobile node receives the packet as if it
were still physically part of the private network. The

process of chained registration lends a topological
credibility to the mobile node with regard to the private
network which the mobile node had lost by being physically
outside the private network.

Figure 3 is a diagram illustrating the extensibility of
a chained registration technique.

In the chain of registrations described above with
respect to Figures 1 and 2, two separate "tunnel segments"
are created to compose the compound tunnel between the
mobile node and the home agent. The first tunnel segment is
created between the FA and the gateway while the second is
composed between gateway and home agent. A chained
registration is possible with many such tunnel segments, as
shown in Figure 3. The tunnel between home agent and mobile
node is composed of N tunnel segments. Each segment
starting node may pre-pend an addressing header which is
then stripped by the segment ending node to recover the
original packet header.

Figure 4 is a flowchart of the chained registration
technique according to at least one embodiment of the
invention.

According to step 400, the first step in chained
registration is that the MN (mobile node) should compose a
registration request on its own behalf. If the home agent
is reached, i.e., if the registration request indicates that
the destination address is true home agent (step 410) then
and only then would a registration reply be provided (step
440). If not, then according to step 420, the registration
chain will be composed by the tunnel segment. Each tunnel
segment will in turn compose registrations "chaining" their
way until the home agent is reached (checked at step 410).
When each registration chain is composed, the next segment
will unwrap the registration to check for the home agent as
the destination address. When the home agent is reached, a
registration reply is provided (step 440).

After the registration reply is provided, it is checked
for completeness by accessing certain fields and headers

(step 450). If not, then the home agent will provide back to the mobile node the codes and information necessary to form a complete registration request. Such information may include the home address for the mobile node or discovery of a dynamic home agent address (step 460). If all registration fields are complete (checked at step 450), then the registration process is also considered complete (step 470).

SECURITY

Authenticating Registrations

In the example above, a second registration was created by the gateway and sent to the home agent. From the home agent's point of view, this registration request is the same as what it would have received from the MN directly; the mobile node is considered to be "at" the gateway.

However, from the standpoint of security, it may be desirable to make explicit which network entity composes the packet. This dictates which security association is used to verify the authentication field in the registration. For instance, a registration request composed by the mobile node to its home agent directly should be authenticated using a security association common to those two entities. On the other hand, a surrogate registration request composed by the gateway to the home agent on behalf of the MN, should be authenticated using a security association common to the gateway and the home agent.

The creator of the registration request should be provided with a mechanism to indicate which security association should be used. For example, registration request composed by the gateway on behalf of the mobile node looks just like one issued by the mobile node itself.

An "SPI" (Security Parameters Index) has been provided in the mobile IP standard to refer to the security association with which a packet must be processed at the destination node and defines which security association is to be used between systems.

The SPI is an arbitrary 32-bit value that identifies the security association for a datagram, relative to the destination IP address (such as the mobile node IP) contained in the IP header with which this security header is associated, and relative to the security protocol (such as chained mobile registration) employed. A security association can be guaranteed by referring to the SPI, the destination address and the security protocol.

Figure 5 illustrates a registration request and reply over the Internet according to one embodiment of the invention.

When a mobile node tries to register over the Internet, it may not know its home IP address, because it is booting a new TCP/IP session instead of resuming an already active one, or because its home IP address is dynamically assigned by the private net through DHCP (Dynamic Host Control Protocol). The mobile node might have obtained a new IP address by using an extended registration request. The requirement for remote booting might be to obtain an IP address from its "home" subnetwork, with the understanding that each remote boot could produce a different one. Network computers, for instance, typically are assigned an IP address upon booting, which is only valid for that boot session.

What is needed is a home IP address discovery mechanism akin to the home agent IP address discovery mechanism. In both cases, a registration denial would carry the necessary information. In order to achieve home IP address discovery, the invention, in one embodiment, defines a new error code: "invalid home address." "Invalid home address" can include both cases where:

1. The mobile node requires an address assignment from the subnet; or

2. The mobile node's lease (time for which use of the IP address was granted) on its previous address has expired.

In the "co-located" case where the MN is also its own
FA, the MN temporarily acquires a topologically significant
COA for use as a tunnel endpoint and thus the mobile node is
directly addressable by the home agent and has a
topologically significant COA address.   In the co-located
case,

```
            Assume:
               *1.   the home prefix is known
                2.   HA prefix is known
                3.   secret is known
                4.   care-of address is known
               *5.   care-of address is co-located

        In this case, what is desired is:
                1.   MN home address
```

The home agent discovers that the home address field is
not completely filled out, obtains a new address within the
indicated prefix and returns that to the mobile node using
the below reply.   It is also possible to discover both the
home agent and the mobile node address.

```
            Assume:
               *1.   the home prefix is known
               *2.   HA prefix is known
                3.   secret is known
                4.   care-of address is known
               *5.   care-of address is co-located

        Want:
                1.   HA address
                2.   MN home address
```

In each case, the registration request fields would
contain:

```
                :
                :
            Home Address = the mobile node's home prefix
            Home Agent = directed broadcast to HA's prefix
            Care-of Address = co-located care-of address
```

In this registration request the home IP address (for
the mobile node) has only the home prefix, and is thus an
incomplete address.   Recognizing this, the home agent will
return the home IP address.   However, before the home agent
can do any assigning or passing of IP addresses back to the

mobile node, the home agent address may also need to be discovered. An initial reply with code 136 (unknown home agent address) tells the mobile node which home agent to use. Subsequently, the mobile node may discover its own home address. The MN must first discover the home agent address because the latter must be willing to provide some address allocation services on the mobile node's behalf.

In another case, where there is no co-location, but a separate foreign agent,

```
Assume:
  *1.  the home prefix is known
  *2.  HA prefix is known
   3.  secret is known
   4.  care-of address is known
```

In this case, the foreign agent uses the identification field to determine which mobile node to send replies to. It is presumed that a foreign agent learn the mobile node MAC (Medium Access Control) address (which is a link layer address such as an ethernet address) from snooping the registration request. Nevertheless, it is difficult to implement a mobile node that sends registration requests (or any other traffic) before configuring its own address. Because of this, the co-located case is easier to implement, and would work very well over PPP (Point-to-Point Protocol).

The exemplary embodiments described herein are provided merely to illustrate the principles of the invention and should not be construed as limiting the scope of the invention. Rather, the principles of the invention may be applied to a wide range of systems to achieve the advantages described herein and to achieve other advantages or to satisfy other objectives as well.

CLAIMS:

What is claimed is:

1.   A method for establishing remote access of a
mobile node to a private network comprising:
    composing a plurality of tunnel segments between said
mobile node and said private network, each tunnel segment
having a source endpoint and a destination endpoint;
    composing by the tunnel segments a plurality of
registration requests, one or more tunnel segments prefixing
an address for said source endpoint and an address for said
destination processing said registration requests in
succession until a secure data transfer pathway is created
between mobile node and private network.

2.   A method according to claim 1 wherein said data
transfer pathway has the home agent as its endpoint in the
private network.

3.   A method according to claim 1 further comprising
discovery of the home address of said mobile node.

4.   A method according to claim 2 further comprising
discovery of the home agent address.

5.   A method according to claim 1 wherein said
composing a plurality of registration requests includes:
    each tunnel segment composing a chain of the
registration request; and
    unwrapping of the tunnel segment composed request at
the next tunnel segment until reaching the home agent.

6.   A method according to claim 5 further comprising:
    providing a registration reply upon reaching said home
agent;

13

if all registration fields are not complete then sending back to said mobile node the information and codes to complete a full registration request; and

if all registration fields are complete, establishing a secure data transfer pathway.

7.   A method according to claim 6 wherein said composing registration requests by tunnel is repeated with said full registration request.

8.   A method according to claim 1 wherein one tunnel segment is composed by a foreign agent acting between said mobile node and said private network.
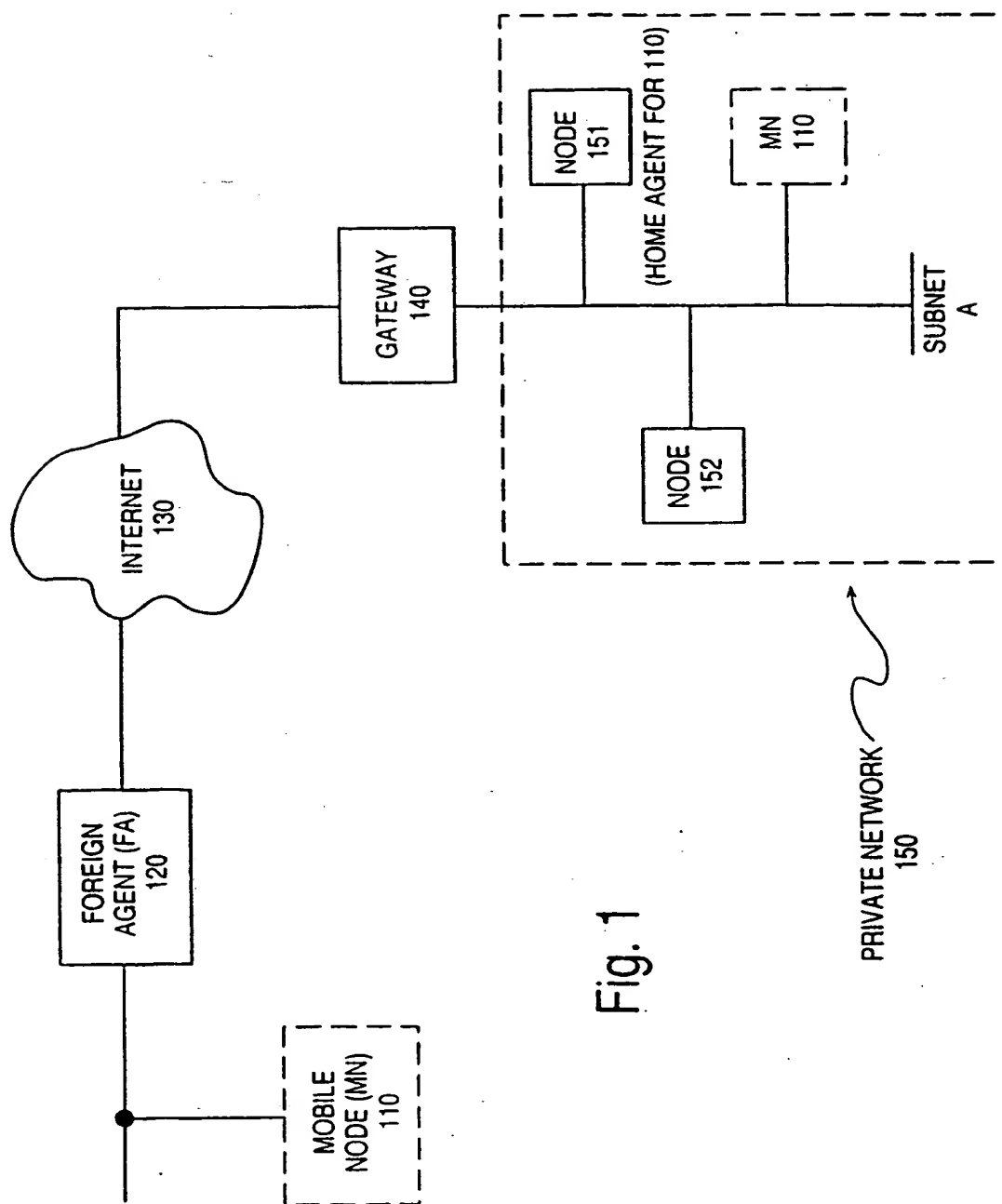
1/4

Fig. 1

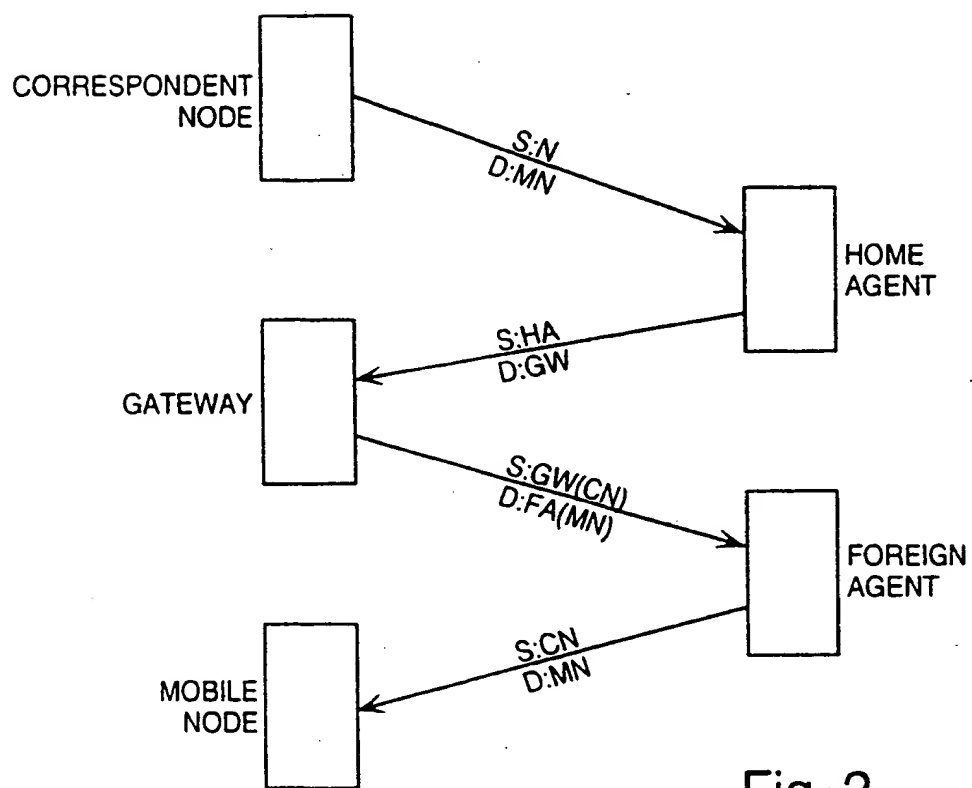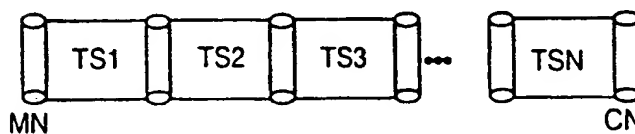2 / 4

REPRESENTATIVE DATA FLOW DIAGRAM

Fig. 2

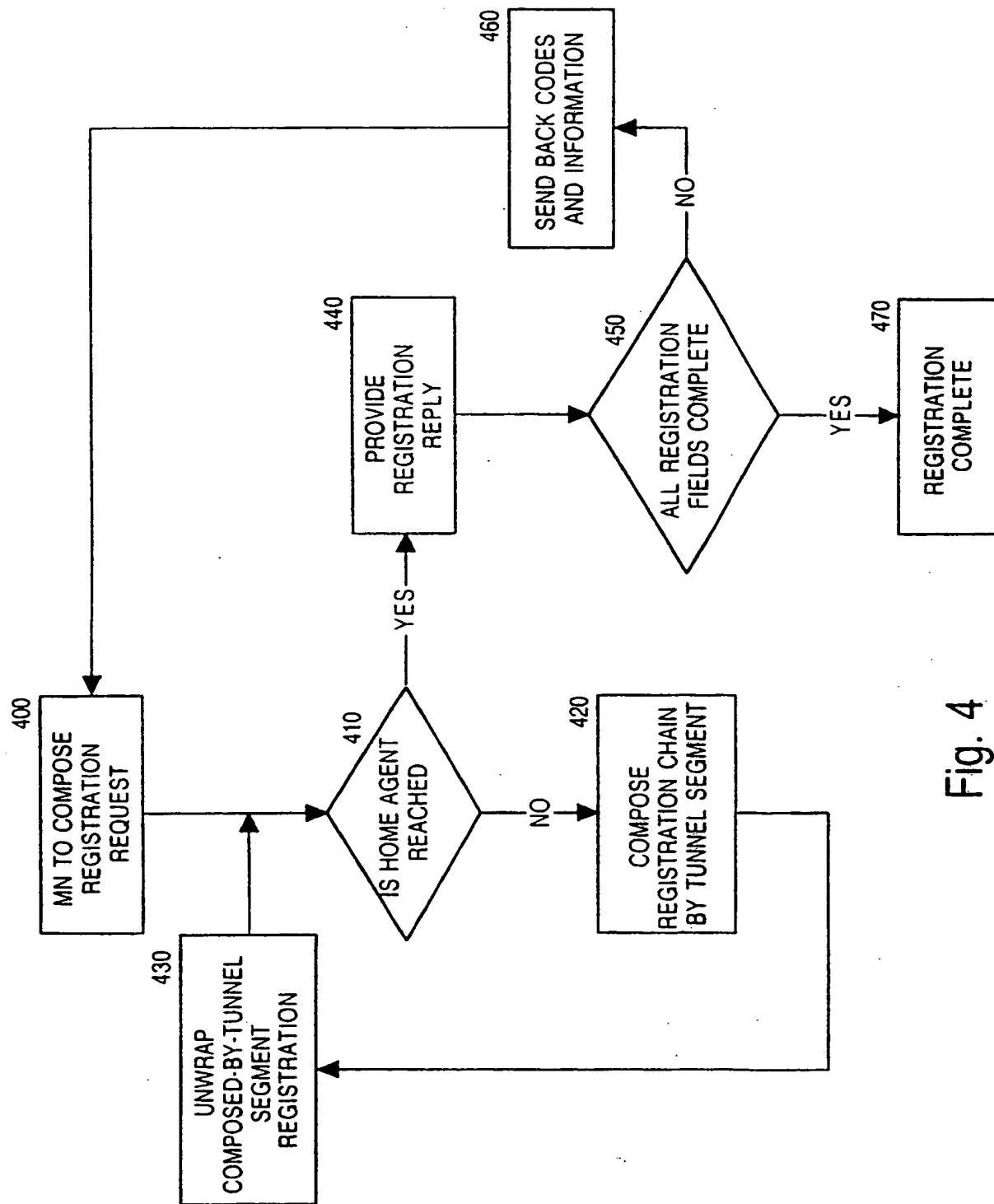

Fig. 3

Fig. 4

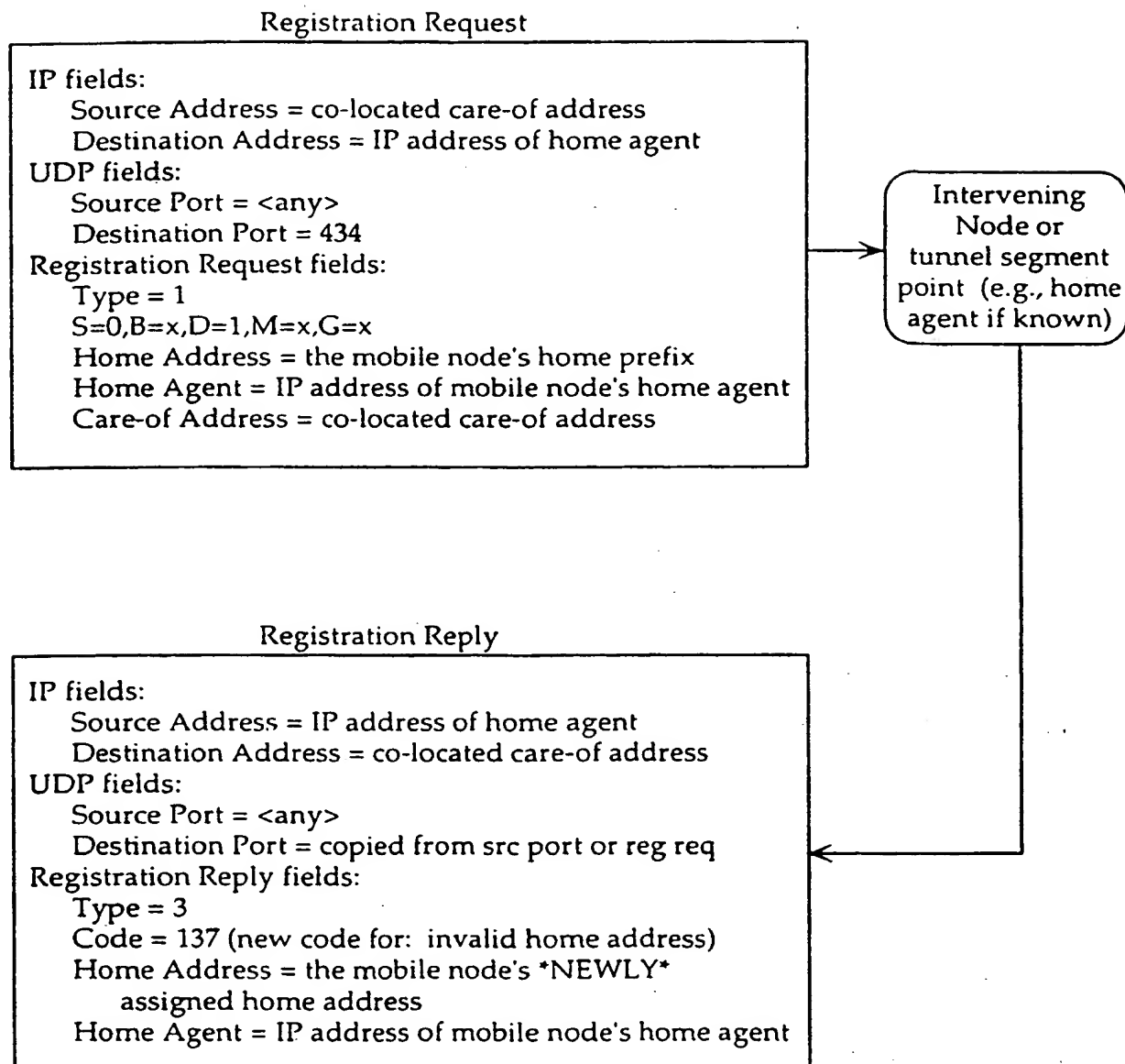Registration Request

```
IP fields:
    Source Address = co-located care-of address
    Destination Address = IP address of home agent
UDP fields:
    Source Port = <any>
    Destination Port = 434
Registration Request fields:
    Type = 1
    S=0,B=x,D=1,M=x,G=x
    Home Address = the mobile node's home prefix
    Home Agent = IP address of mobile node's home agent
    Care-of Address = co-located care-of address
```

Intervening
Node or
tunnel segment
point (e.g., home
agent if known)

Registration Reply

```
IP fields:
    Source Address = IP address of home agent
    Destination Address = co-located care-of address
UDP fields:
    Source Port = <any>
    Destination Port = copied from src port or reg req
Registration Reply fields:
    Type = 3
    Code = 137 (new code for: invalid home address)
    Home Address = the mobile node's *NEWLY*
        assigned home address
    Home Agent = IP address of mobile node's home agent
```

Fig. 5

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L29/06   H04L29/12   H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	INOUE A ET AL: "IP LAYER SECURITY AND MOBILITY SUPPORT DESIGN POLICY AND AN IMPLEMENTATION" ISS. WORLD TELECOMMUNICATIONS CONGRESS. (INTERNATIONAL SWITCHING SYMPOSIUM),CA,TORONTO, PINNACLE GROUP, page 571-577 XP000720565	1,2,5-8
Y	abstract page 571, left-hand column, line 1 -page 576, left-hand column, line 14 ---	3,4
Y	WO 98 32301 A (ERICSSON TELEFON AB L M) 23 July 1998 (1998-07-23) abstract page 1, line 1-31 page 2, line 29 -page 6, line 20 page 8, line 5 -page 17, line 20 ---	3

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

5 January 2000

Date of mailing of the international search report

27/01/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,
Fax: (+31–70) 340–3016

Authorized officer

Lievens, K

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	GIOVANARDI A ET AL: "TRANSPARENT MOBILE IP: AN APPROACH AND IMPLEMENTATION" GLOBAL TELECOMMUNICATIONS CONFERENCE (GLOBECOM),US,NEW YORK, IEEE, page 1861-1865 XP002068554 ISBN: 0-7803-4199-6 page 1861, left-hand column, line 1 -page 1863, left-hand column, line 11 ---	4
A	LI Y ET AL: "PROTOCOL ARCHITECTURE FOR UNIVERSAL PERSONAL COMPUTING" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS,US,IEEE INC. NEW YORK, vol. 15, no. 8, page 1467-1476 XP000721278 ISSN: 0733-8716 page 1467, left-hand column, line 1 -page 1468, left-hand column, line 37 page 1469, right-hand column, line 8 -page 1472, left-hand column, line 36 -----	6,8

3

INTERNATIONAL SEARCH REPORT

Information on patent family members

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9832301 A	23-07-1998	AU 5684698 A EP 0953265 A	07-08-1998 03-11-1999

THIS PAGE BLANK (USPTO)